Router and Node Configuration

Introduction

A CWM network management system consists of the following components (see Figure 10-1).

- CWM workstations (server, clients, and statistics collectors)
- Routers (acting as intermediaries between CWM and the managed network)
- Nodes that make up the managed network

![Figure 10-1 Network Management Components]

CWM workstations together provide network management by performing the following functions.

- Discover the network topology using AutoRoute and/or PNNI ILMI
- Manage MIB objects using SNMP
- Collect statistics using FTP and TFTP.
- Handle traps from managed nodes.

For these functions to perform correctly, all components in the network management system must be properly configured. This requirement includes configuration of CWM workstation file, routers, and the managed network’s nodes.
This chapter provides details of how to configure:

- The routers that connect CWM to the network and
- The managed network nodes themselves.

Configuration details for CWM servers are provided in Chapters 3 and 4, configuration details for Statistics Collectors and Managers are provided in Chapters 7 and 8 and Appendix A.

**Note**

The procedures in this chapter assume the use of the Cisco Command Line Interface (CLI) for node configuration. Some of these commands contain parameters that are not concerned with CWM and network management and, as such, these parameters are not discussed in this chapter.

Full details of all node commands can be found in the appropriate command reference (see the “Related Documentation” section in the Preface of this Installation Guide).

The procedures described in this chapter should be performed BEFORE CWM is launched for the first time. Once CWM is launched, the Graphical User Interface (GUI) can be used to add to or modify many of the configuration parameters set in these procedures.

### Configuring Routers

In the context of CWM, routers act as intermediaries between the CWM workstations and the managed network nodes, see Figure 10-1.

Routers need to be configured for an ATM interface on the network side and for a LAN (Ethernet) interface on the CWM side.

#### ATM Network Side

To configure the ATM interface to the gateway node, you need to perform the following tasks:

**Step 1** Create an ATM interface.

**Step 2** Assign an IP address for the ATM interface.

**Step 3** Assign an ATM address (AES A) for the ATM interface.

**Step 4** Configure the ATM interface to be the ATMARP server for the gateway node.

**Step 5** Enable and configure ILMI

#### LAN Ethernet Side

If the router’s IP address for the ATM interface is on the same subnet as the IP address on the node’s ATM interface, no additional configuration is required for the router’s IP LAN interface.
If not, you need to perform the following tasks to configure the IP interface to the LAN.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Manually configure the IP host-route for each Cisco MGX 8850 to which the interface will connect.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Configure a routing protocol to broadcast the switch IP addresses to the LAN or create default routes to the switch on the management workstation.</td>
</tr>
</tbody>
</table>

The specific procedure used to configure the ATM router will depend upon the router type. The following example shows the IOS commands used to configure a Cisco 7204 router to support IP over ATM communications with the Cisco MGX 8850.

**Example 10-1  Router Configuration Commands for IP Communications over ATM**

```
config term  # Enters global configuration mode
ip routing#enables ip routing
ip route 0.0.0.0 0.0.0.0 W.X.Y.Z 1 (set default route)
interface atm 0
ip address A.B.C.D G.H.I.J  # G.H.I.J = netmask
atm nsap-address 47.0091.8100.0000.0010.7b65.f258.0010.7b65.fffe.f1
atm uni-version 3.1
atm pvc 1 0 5 gsaal
atm pvc 2 0 16 ilmi #Optional. Enter to enable ILMI.
atm ilmi-keepalive 10 #Optional. Enter to configure ILMI.
atm esi-address 00107B65FFFF.F1 #Optional. Enter to support ILMI.
atm arp-server self
no shut
^Z
```

**Configuring Managed Network Nodes**

The tasks involved in configuring the network nodes fall broadly into the following categories.

- Assigning IP addresses
- Setting up ATM connections
- Enabling ATM ILMI
- Setting up community strings
- Setting up statistics collection
- Setting up trap management

The precise procedures for performing these tasks vary depending on the node device type. Node device types in this chapter are categorized as:

- IGX and BPX nodes
- BPX/SES nodes
- MGX nodes
Assigning IP Addresses

All managed nodes require addresses by which they can be identified and reached. Depending upon the node type, addresses are a combination of one or more of the following.

- A LAN IP address
- A network IP address
- An ATM address

IGX and BPX Nodes

**Step 1** Assign an IP address for use by CWM.

For inband communications, use the `cnfnwip` command to assign a network IP address. The syntax for this command is,

```
cnfnwip <IPAddr> <IPSubmask>
```

For out-of-band communications, use the `cnflan` command to assign a LAN IP address. The syntax for this command is,

```
cnflan <IP_Address> <IP_Subnet_Mask> <Maximum LAN Transit Unit> <TCP Service Port>
```

The TCP service port should be entered as 5120.

BPX/SES Nodes

**Step 1** Check that the IP addresses for the BPX node have been set up as described in the previous section.

**Step 2** In the SES, use the `ipifconfig` command to setup the IP address

This command is used to assign both a LAN IP address and a Network IP address.

For inband communications assign a Network IP address. The command syntax is:

```
ipifconfig atm0 [ <ip_address> ] [ netmask <mask> ] [ broadcast <broad_addr> ]
[ dest <peer_ip_address> ] [ up | down ] [arp | noarp][svc | nosvc] [pvc | nopvc] [ default | nodefault]
[clrstats]
```

For out-of-band communications, assign a LAN IP address. The command syntax is

```
ipifconfig lnPci0 [ <ip_address> ] [ netmask <mask> ] [ broadcast <broad_addr> ]
[ dest <peer_ip_address> ] [ up | down ] [arp | noarp][svc | nosvc] [pvc | nopvc] [ default | nodefault]
[clrstats]
```

Enter the IP address to be assigned and its netmask in the first two parameters.

**Step 3** Use to `cnfndparms` command, option 7, to specify which IP address is to be used with CWM. The format of this command is:
cnfndparms 7 <option_value>

In the option_value field, enter the value to be used as follows:

0: The atm0 interface will be the primary.
1: No interface will be used. This prevents ILMI Node Discovery.
2: The lnPci0 interface will be the primary.

### MGX nodes

Use the following procedure to assign IP addresses to MGX nodes.

**Step 1**

For inband communications assign a Network IP address. The command format is:

```
ipifconfig atm0 [ <ip_address> ] [ netmask <mask> ] [ broadcast <broadcast_addr> ]
[ dest <peer_ip_address> ] [ up | down ] [arp | noarp] [svc | nosvc] [pvc | nopvc] [ default | nodefault] [clrstats]
```

For out-of-band communications, assign a LAN IP address. The command format is

```
ipifconfig lnPci0 [ <ip_address> ] [ netmask <mask> ] [ broadcast <broadcast_addr> ]
[ dest <peer_ip_address> ] [ up | down ] [arp | noarp] [svc | nosvc] [pvc | nopvc] [ default | nodefault] [clrstats]
```

In the first two parameters, enter the IP address to be assigned and its netmask.

**Step 2**

Use to `cnfndparms` command, option 8, to specify which IP address is to be used with CWM. The format of this command is:

```
 cnfndparms 8 <option_value>
```

In the option_value field, enter the value to be used as follows:

0: The atm0 interface will be the primary.
1: No interface will be used. This prevents ILMI Node Discovery.
2: The lnPci0 interface will be the primary.

### Setting up ATM Connections

Except for completely out-of-band LAN based network management, all nodes must be configured so that ATM connections can be established between CWM workstations and the managed nodes. Usually this consists of setting up the correct node interfaces that are used for CWM/node communication.

**Note**

Regardless or whether inband or out-of-band is used, all nodes must also have ATM connections to carry non-CWM regular network traffic.
IGX and BPX Nodes

IGX nodes and BPX nodes (not equipped with an SES), use the Cisco proprietary Link0/Link1 and AutoRoute protocols for network discovery and CWM connectivity. Under this scheme one node can be designated as a gateway node to provide CWM connectivity to all the other similar nodes. Alternatively CWM can communicate directly with each managed node. The user specifies which method is to be used in the network.conf file in the CWM server workstation.

Configure each node as follows:

Step 1
Check that the node has its IP addresses assigned correctly. If not, use the \texttt{cnflan} or \texttt{cnfnwip} commands as appropriate (see above).

Step 2
Use the \texttt{cnfname} command to assign a node name. The command format is:

\begin{verbatim}
 cnfname <nodename>
\end{verbatim}

BPX/SES Nodes

Step 1
Check that the BPX has a nodename (see previous section).

Step 2
On the SES, check that its IP addresses are assigned correctly. If not, use the \texttt{ipifconfig} and \texttt{cnfndparms} commands as appropriate (see above).

Use the following steps to configure the SES to be a PNNI controller for the BPX.

Step 3
Enter the \texttt{cnfpnni-node -enable false} command to disable the node index.

Step 4
Enter the \texttt{addpnni-node} command and set the desired PNNI parameters. See the SES Command Reference for details.

Step 5
Enter the \texttt{cnfpnni-node -enable true} command to enable the node index.

Use the following steps to create and configure a PNNI port.

Step 6
On the SES PXM card, enter the \texttt{addpnport} command to create a pnni port. The command format is:

\begin{verbatim}
 addpnport <slot number><port number>
\end{verbatim}

Step 7
Enter the \texttt{dnpnport} command to down the port. This is required to configure the port. The format of the command is:

\begin{verbatim}
 dnpnport <slot number><port number>
\end{verbatim}

Step 8
Enter the \texttt{cnfpnportsig} command to configure the type of signalling on the port. The format of the command is:

\begin{verbatim}
 cnfpnportsig <slot number><port number> -nniver pnni10
\end{verbatim}

This command configures the port for NNI with PNNI version 10 signalling

Step 9
Enter the \texttt{uppnport} command to activate the port. The format of the command is:

\begin{verbatim}
 uppnport <slot number><port number>
\end{verbatim}

MGX nodes

ATM connections extend node management to all CWM workstations that have access to the ATM network in which the node is installed.

To support the ATM SVCs over which the IP traffic travels, both the router and nodes are configured to map the respective IP addresses to ATM End Station Addresses (AESAs). When a management session is initiated, the IP workstation directs all communications to the IP address assigned to the ATM interface on the node. The router encapsulates this IP traffic in ATM cells and forwards it over SVCs to the node. The destination node retrieves the IP messages from the ATM cells and forwards them to the internal IP management tools. Replies to the workstation follow the same path in reverse.

Any workstation with a connection to a properly-configured ATM router can manage any node in the network. Furthermore, additional routers connected to other nodes can be configured to support this feature, enabling node configuration from multiple locations throughout an ATM network.

To support IP connectivity over the ATM interface, perform the following tasks:

- Assign an IP address to the ATM interface.
- Assign an AESA to the ATM interface.
- Define an AESA for every adjacent router that supports IP communications to the ATM interface.
- Configure ATM communications between the node and the router.

To configure the node to support IP connectivity to the ATM interface, use the following procedure.

**Step 1** Check that the MGX node has an assigned network IP address and netmask. Use the `ifipconfig atm0` command to assign such an address and mask if necessary (see Assigning IP Addresses above for details).

**Step 2** Enter the `svcifconfig` command to configure the node AESA (ATM address) for IP connectivity. The format of this command is:

```
svcifconfig <interface> <router | local> <svc_address> [atmarp | noatmarp] [llcencap | vcmux] [default | nodefault] [reset] [delete][force] [clrstats]
```

Specify `atm0` for the interface parameter and specify `local` for the router|local parameter. Enter the assigned ATM address for the node in the `svc_address` parameter. This address must conform to the address plan for the node. The command becomes:

```
svcifconfig atm0 local <svc_address>.
```

**Step 3** Enter the svcifconfig command again to define the ATM address of the router.

Specify router for the router|local parameter and enter the router’s address.

```
svcifconfig atm0 router <ATM_Addr>
```

**Step 4** If not already configured, configure the PNNI controller.

Use the `addcontroller` command to configure the PNNI controller. The format of this command is:

```
addcontroller <cntrlrId> i <cntrlrType> <slot> [cntrlrName]
```

`cntrlrId` cntrlrType should both be specified as 2 (PNNI)

**Step 5** Configure the controller using the `cnfpnni-node` command. This command is used to configure values for peer level, peer group ID, peer node address, and peer node ID.
For more details of the **addcontroller** and **cnfpnni-node** commands, refer to *Cisco MGX 8850 Software Configuration Guide Release 5.1*.

**Step 6** Configure an ATM line and port to the ATM router. The sequence of commands is:

- `upln` - bring up a line to the router.
- `cnfln` - if necessary, specify more configuration values for the line.
- `addport` - add a port to the line, specify UNI for the interface type and an SCT of 6.
- `cnfport` - if necessary, specify more configuration values for the port.
- `addpart` - add a partition of type PNNI and support for at least 20 connections.
- `upport` - bring up the port.

For more details see “Configuration Quickstart” in Chapter 5, “Provisioning AXSM Lines and Cards for Communication” in the *Cisco MGX 8850 Software Configuration Guide, Release 5.1*.

**Step 7** Enter the **dsppnysaddr** command to verify connectivity to directly attached ATM routers.

The ATM addresses of directly attached ATM routers should appear in the list the node displays. To display an ATM address for a remote router, you need to establish a CLI session on the remote node and enter the **dsppnysaddr** command.

**Step 8** Enter the **dsppnports** command to check the status of ports leading to directly-attached ATM routers.

The following example shows commands that you can use to configure an Cisco MGX 8850 for IP communications over ATM.

### Example 10-2 Node Commands for IP Communications over ATM

```plaintext
mgx8850a.7.PXM.a> ipifconfig atm0 A.B.E.F  # Replace A.B.E.F with IP Address
mgx8850a.7.PXM.a> svcifconfig atm0 local 47.0091.8100.0000.0010.7b65.f258.0010.7b65.1111.01
mgx8850a.7.PXM.a> svcifconfig atm0 router 47.0091.8100.0000.0010.7b65.f258.0010.7b65.ffff.ffff.e1
mgx8850a.7.PXM.a> addcontroller 2 l 2 7  #if controller does not already exist
mgx8850a.10.AXSM.a > upln 1.1
mgx8850a.10.AXSM.a > addport 1 1.1 96000 96000 6 1
mgx8850a.10.AXSM.a > addpart 1 1 2 500000 500000 500000 500000 1 20 32 52 1 20
mgx8850a.10.AXSM.a > upport 1
mgx8850a.10.AXSM.a > cnfifmi -if 1 -id 1 -ilmi 1 -vpi 0 -vci 16 -trap 1 -s 10 -t 10 -k 10
#Optional. This command configures ILMI for the port.
mgx8850a.7.PXM.a> dsppnysaddr
(example output)
47.0091.8100.0000.0010.7b65.f258.0010.7b65.ffff/152
Type:      uni     Port id:   17111041

mgx8850a.7.PXM.a> dsppnports
(example output)
Per-port status summary

<table>
<thead>
<tr>
<th>PortId</th>
<th>IF status</th>
<th>Admin status</th>
<th>ILMI state</th>
<th>Total Activeconns</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:1.1:1</td>
<td>up</td>
<td>up</td>
<td>Undefined</td>
<td>3</td>
</tr>
</tbody>
</table>
```

For more details of the **addcontroller** and **cnfpnni-node** commands, refer to *Cisco MGX 8850 Software Configuration Guide Release 5.1*.
Enabling ATM ILMI

IGX and BPX Nodes

**Step 1** Use the ATM `cnfport` command protocol parameter to enable ILMI (or XLMI in the case of hybrid networks). Set the advertise interface information parameter to Yes. This parameter defines whether the interface is authorized to advertise its interface information. Values are Y/N. The default is Y.

**Step 2** Use the configure node parameters command, `cnfnodemparm`, to specify which IP address is to be used by CWM. Set option 56 in this command to NW or Lan as appropriate. This option specifies whether to use the configured LAN IP or network IP address as the management IP address used in the ILMI Neighbor Discovery procedure.

BPX/SES Nodes

**Step 1** Set up the configuration on the BPX as described in the previous section.

**Step 2** On the SES use the `dnpnport` command to de-activate a PNNI port.

**Step 3** On the SES use the `cnfilmienable` command to enable ILMI on a PNNI port.

MGX nodes

All ports on MGX nodes that are used for PNNI discovery must be ILMI enabled.

Use the `cnfilmi` command. The format of this command is:

```
  cnfilmi <ifNum> -id <partitionID> -ilmi <ilmiEnable> -vpi <vpi> -vci <vci> -trap <ilmiTrapEnable> -s <keepAliveInt> -t<pollingIntervalT491> -k <pollInctFact>
```

Make the partition ID the same as that for the port set up to communicate with the router. Set both of the `ilmiEnable` and `ilmiTrapEnable` parameters to enable. The standard vpi and vci numbers for PNNI ILMI are 0 and 16 respectively.

Setting up Community Strings

The SNMP protocol requires that an SNMP manager provides a correct community string before an SNMP agent in the node will respond to a GET or SET command. SNMP community strings must be configured at each node and the corresponding strings must be configured in the SNMP manager in the CWM Server.

Two string types can be configured:

- One for read only privileges (for GET commands), with a default of “public”.
- One for read/write privileges (for SET and TRAP commands), with a default of “private”.

The SNMP rules for community strings are:

- Up to 32 characters in length
- Strings cannot contain a blank space, an “@,” or a quote (”) character.
Reserved strings are:
- Community rw string: “private”
- Community ro: “public”

**IGX and BPX Nodes**

**Step 1**
Use the `cnfsnmp` command to configure the node’s SNMP community string. This command has the syntax:
```
cnfsnmp <GET community string> <SET community string>
```

Enter the community strings as appropriate. If strings are not provided, the defaults are used.

**BPX/SES Nodes**

**Step 1**
Check that the community strings for the BPX have been configured (see previous section).

**Step 2**
On the SES, use the `cnfsnmp` command to set the community strings for the SES. The syntax of this command is:
```
cnfsnmp <GET community string> <SET community string>
```

Enter the GET (read only) community string and the SET (read/write) community strings. Traps will use the SET community string.

**MGX nodes**

Use the `cnfsnmp` command to set the community strings. This command also allows the user to specify the SNMP values for contact and location. Depending upon the use of this command, it has three forms as follows:
```
cnfsnmp community string [ro | rw]
```
```
cnfsnmp contact string
```
```
cnfsnmp location string
```

The `cnfsnmp community` form of the command allows the specification of both read only (ro) and read/write (rw) community strings but only one string can be specified in a single command. To specify both ro and rw strings, the command must be executed twice.
Setting up Statistics Collection

IGX and BPX Nodes

Use the following procedure to setup statistics collection on IGX and BPX nodes.

**Step 1**
Use the `cnfcdparm` command to configure the multichannel statistics feature.

This feature is supported on the BPX and IGX platforms, for BXM and UXM cards. It enables the nodes to collect and propagate statistics to a CWM workstation. The channel statistic types vary in number and type based upon the level of support specified in the `cnfcdparm` command. The syntax of this command is:

```
cnfcdparm <slot> <index> <value>
```

*<slot>* is the slot number for which the statistics level is being specified.

*<index>* can be 1, 2, or 3. Enter a value of 1 to signify that multichannel statistics are being specified.

*<value>* specifies the level of statistics to be collected, it can have the value of 0, 1, 2, or 3. Enter the value corresponding to the level of statistics to be collected.

For a description of all four channel statistics levels, see the *BPX 8600 Installation and Configuration Manual Release 9.3.30*, Chapter 5 BXM Card Sets: T3/E3, 155, and 622.

**Step 2**
Use the `cnfstatmast` command to specify the CWM workstation to which statistics are to be sent. The syntax of this command is:

```
cnfstatmast <IP Address>
```

Specify the IP address of the CWM workstation that is collecting statistics for this node.

BPX/SES Nodes

**Step 1**
Check that statistics collection for the BPX has been configured as described in the previous section.

**Step 2**
On the SES, use the `cnfstatsmgr` command to specify the CWM workstation to which statistics are to be sent. The syntax of this command is:

```
cnfstatsmgr <index> <IP Address>
```

*<index>* can have the value of 1, 2, 3, and 4 to indicate type of system associated with the IP address.

1 = Primary statistics manager
2 = Secondary statistics manager
3 = Tertiary statistics manager
4 = Master statistics manager
MGX nodes

**Step 1** Use the `cnfstatsmgr` command to specify the CWM workstation to which statistics are to be sent. The syntax of this command is:

```
cnfstatsmgr <index> <IP Address>
```

<index> can have the value of 1, 2, 3, and 4 to indicate type of system associated with the IP address.

1 = Primary statistics manager
2 = Secondary statistics manager
3 = Tertiary statistics manager
4 = Master statistics manager

**Note** In the current release, index options 1 through 3 are not applicable to the present switch architecture. Use index option 4 to specify the IP address of the statistics master for the switch. This action defines the IP address of the workstation that is authorized to enable or disable statistic on the switch.

Setting up Trap Management

IGX and BPX Nodes

IGX and BPX nodes do not send standard SNMP trap messages to CWM. Instead, these node use a variety of message types to communicate network changes and alarms. These messages are converted to SNMP traps in the CWM workstation where they can be processed along with traps received from other node types. Operating within the Cisco proprietary Link0/Link1 protocol, the following message types are used.

- Events in ASCII string format
- Topology update messages
- Object updates in robust object message format
- Alarms in robust alarm message format

**Note** The term “robust” is used to mean that the protocol contains acknowledgement features to guarantee delivery of the message.

Two commands can be used to configure parameters for robust alarm messages.

`cnfrobparm` (configure robust parameters) and `cnfasm` (configure ASM card)
Use the following procedure to configure robust alarms.

**Step 1**

Use the `cnfrobparm` command to configure parameters associated with the transmission of robust alarms. The syntax of this command is:

```
cnfrobparm <index> <value>
```

Enter values for `<index>` and `<value>` according to Table 10-1

**Table 10-1  Index and Parameter Values for the cnfrobparm command**

<table>
<thead>
<tr>
<th>Index No.</th>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Robust State wakeup timer</td>
<td>The Robust State machine becomes active after the specified time period has elapsed. If this timer value increases, the state machine operates less often and places less load on the controller card. Units of measure are seconds.</td>
<td>10 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Robust update timer</td>
<td>Once a message has gone to the NMS, another message does not go until this timer expires. Units of measure are seconds.</td>
<td>10 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Robust acknowledgment time-out</td>
<td>An acknowledgment must be returned by the NMS within this time period or it is assumed the communications link is down. Units of measure are seconds.</td>
<td>600 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Robust acknowledgment reset timeout</td>
<td>After a downed link has been repaired, the next message goes out after this time period has elapsed. The purpose of this time period is to let the link settle after the repair. Units of measure are seconds.</td>
<td>60 seconds</td>
</tr>
</tbody>
</table>

**Step 2**

Use the `cnfasm` command to configure certain alarm parameters. This command allows the user to set various alarm values and to enable or disable the commands.

When this command is executed, the following list of alarms is displayed. The user responds by entering an alarm number and then changing the value (or status) as necessary.

```
[3] Power B deviation:10 V (49.1)
  ALM
[6] ACO button -  [14] BPX 8600 card slot -
[12] Fan 2 RPMY
[13] Fan 3 RPMY
```
BPX/SES Nodes

Step 1  On the SES use the `cnftrapip` command to configure the address on the SES where the traps are configured before being sent out to the CWM workstation. The syntax for this command is:

```
  cnftrapip <ip address>
```

Enter the IP address of the switch that will be sending the traps to the CWM workstation.

Step 2  Use the `addtrapmgr` command to set up an SNMP manager to receive traps.

The syntax of this command is:

```
  addtrapmgr <ip_addr> <portnum>
```

`<ip_addr>` is the IP address of the CWM workstation to receive the traps.

`<portnum>` is the port number to be used to send traps. The SNMP default port number is 162.

MGX nodes

Step 1  Use the `cnftrapip` command to configure the address on the MGX where the traps are configured before being sent out to the CWM workstation. The syntax for this command is:

```
  cnftrapip <ip address>
```

Enter the IP address of the switch that will be sending the traps to the CWM workstation.

Step 2  Use the `addtrapmgr` command to set up an SNMP manager to receive traps.

The syntax of this command is:

```
  addtrapmgr <ip_addr> <portnum>
```

`<ip_addr>` is the IP address of the CWM workstation to receive the traps.

`<portnum>` is the port number to be used to send traps. The SNMP default port number is 162.

Firewalls and CWM 15.1

Firewalls set up on managed networks and PCs used as clients may affect the Desktop GUI. The following sections describe how to resolve these issues.

Firewall on PC

Problem

If a PC based firewall like BlackIce is used, the protection settings to enable incoming connections may need to be changed. In CWM 15.1, when running a client is running on a remote PC, the server opens new connections when sending node and network updates to the Desktop GUI. If the PC blocks all incoming calls, this will cause the topology map to not appear on the GUI.
Solutions:

Here are some suggested solutions to the problem. Please use any one of them.

Solution 1

Lower the protection level for incoming connections. In Black Ice, for example, the Protection Level should be set to “Cautious: block some unsolicited inbound traffic” instead of the more restrictive “Nervous: block most unsolicited inbound traffic”.

Solution 2

If the firewall software allows, add CWM server machine as a trusted IP address and allow all traffic from the CWM host.

Solution 3

Limit ports used by CWM clients and servers for corba communication and open these ports on the firewall software. The following steps can be executed to set up the ports:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Stop CWM core</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Stop Orbix processes using 'stoporbix2000' script</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add the following line at the end of the /usr/users/svplus/orbix_domain/domains/cwm_&lt;cwm-machine-name&gt;_domain.cfg file on the CWM workstation: policies:iiop:server_address_mode_policy:port_range = “5500:6000”; This will restrict the CWM processes to use ports between 5500 and 6000 for corba communication. This range is enough for up to 20 clients connecting to the CWM simultaneously. If more than 20 clients will be connected CWM at one time, please increase the upper limit as follows: 30 simultaneous clients - 5500:6100 40 simultaneous clients - 5500:6200 50 simultaneous clients - 5500:6300</td>
</tr>
<tr>
<td>Step 4</td>
<td>Start CWM core.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure the firewall to open the above ports in both directions (from CWM to the clients and vice versa). Other than these ports, the firewall also need to allow 3075 and 3094 ports for communication with the Orbix processes.</td>
</tr>
</tbody>
</table>

Note: The above port range can start from any number as required, please note that the number of ports should remain the same as shown above. For example, the port range can be set to 9000:9500 for 20 clients and so on.
Firewall on LAN:

Problem:

If the network where CWM is located has a firewall configured to restrict traffic from both inside the LAN as well as from an outside PC the topology map will not show up in the Desktop GUI.

Solutions:

Here are some suggested solutions to the problem. Please use any one of them.

Solution 1

Use VPN tunneling for the remote PCs to connect to the CWM machines in the lab

Solution 2

Set up trusted IP addresses in the Firewall. Both CWM machines and the remote PC that are going to use CWM GUI need to be added as trusted IP addresses in the firewall configuration.

Solution 3

Limit ports used by CWM clients and servers for Orbix communication and open these ports on the firewall software. The following steps can be executed to setup the ports:

---

**Step 1**
Stop CWM core

**Step 2**
Stop Orbix processes using 'stoporbix2000' script

**Step 3**
Add the following line at the end of the
/usr/users/svplus/orbix_domain/domains/cwm_<cwm-machine-name>_domain.cfg file on the CWM workstation:

```
policies:iiop:server_address_mode_policy:port_range = "5500:6000";
```

This will restrict the CWM processes to use ports between 5500 and 6000. This range is enough for up to 20 clients connecting to the CWM simultaneously. If more than 20 clients will be connected CWM at one time, please increase the upper limit as follows:

- 30 simultaneous clients - 5500:6100
- 40 simultaneous clients - 5500:6200
- 50 simultaneous clients - 5500:6300

**Step 4**
Start CWM core.

**Step 5**
Configure the firewall to open the above ports in both directions (from CWM to clients and vice versa). Other than these ports, the firewall also need to allow 3075 and 3094 ports for communication with the Orbix processes.

---

**Note**
The above port range can start from any number as required, please note that the number of ports should remain the same as shown above. For example, the port range can be set to 9000:9500 for 20 clients and so on.